VIGYÁZAT! SMS-BEN ÉRKEZHET A KÁRTÉKONY KÓD

A csalók csomagküldő szolgáltatók nevében küldenek üzeneteket.

A karantén-szabályok életbe lépése óta jelentősen megemelkedett az internetes vásárlások, valamint a csomagküldő szolgáltatók általi kézbesítések száma. A helyzet új lehetőséget teremtett a kiberbűnözőknek arra, hogy személyes adatokat szerezzenek meg, kompromittálják az elektronikus kommunikációt, és ezek felhasználásával további bűncselekményeket kövessenek el.

Az elmúlt napokban több lakossági bejelentést is érkezett a rendőrségre olyan SMS-üzenetekre hivatkozva, melyben a címzettet egy csomagküldemény rövid időn belüli érkezésére emlékeztetik. Az üzenet egy linket tartalmaz, amelyet megnyitva valamely csomagküldő szolgálat arculati elemeivel ellátott weboldal jelenik meg, azonban ott semmilyen funkció nem érhető el. Az oldal egyetlen célja, hogy az óvatlan látogató telefonjára vagy más okoseszközére egy kártékony kódot tartalmazó alkalmazást telepítsen, melynek segítségével az elkövetők hozzáférhetnek az eszközön tárolt adatokhoz. A támadás elsősorban Android-rendszert futtató eszközöket érint, melyeken települést követően az alkalmazás akár a netbank-applikációban tárolt adatokhoz is hozzáférhet.

Az áldozattá válás elkerülése érdekében fogadják meg az alábbi tanácsokat!

A támadás megelőzése céljából minden esetben ellenőrizze, hogy valóban attól a csomagküldő-szolgáltatótól kapja-e az értesítést, amelytől a csomagot várja!

Vegye figyelembe azt is, hogy a csomagküldő szolgáltatók saját, hivatalos weblapjukra irányítják át a felhasználókat a csomagkövetési rendszer eléréséhez! A legtöbb esetben a szolgáltatók közvetlenül az üzenetben is tájékoztatják a csomagkézbesítés várható időpontjáról, azt nem szükséges külön felületen ellenőrizni.

Az üzenetben érkezett hivatkozásra kattintás előtt minden esetben érdemes megtekinteni, hogy milyen címen nyílik meg az adott tartalom, és amennyiben ez már látszólag is eltér a szolgáltató valós oldalától, azt mielőbb zárják be! Az androidos eszközökön nem javasolt az ismeretlen forrásból származó alkalmazások telepítésének engedélyezése. Ezen kívül célszerű lehet valamilyen biztonsági szoftver használata is, amely automatikusan blokkolja a kártékony tartalmak elérését.